UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,303	11/21/2003	Michael Bensimon	886-011604-US(PAR)	3004

2512 7590 04/17/2008

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/719,303	BENSIMON ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to remarks and amendment filed on December 26, 2007. Original application contains claim 1-21. Applicant currently amended claims 1-3, 5-10, 13-18, 20-21, and added a new claim 22. The amendment filed have been entered and made of record. Therefore, presently Claims 1-22 are pending for further consideration.

Response to Arguments

Applicant's arguments filed December 26, 2007 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-21 applicant argued that the cited prior art (CPA) [Julin et al. U. S. Patent 5,557,679] does not disclose "*establishing a trust relationship between a radio-communication terminal and a SIM card, in order to secure exchanges between these two entities*".

This is not found persuasive. Cited prior art clearly teaches system and method of a mobile telephone system using personalized active card connected to system central computer via communication network with card identity and authentication to point terminal equipment. The mobile telephone system has a central computer which via a data communication network communicates with a number of after-sales points connected to a customer service. Each after-

sales point has a data terminal equipment connected to a reader for an SIM card and a line coding equipment consisting of a reader an active after-sales card. A keyboard for feed-in of a PIN code into the actual SIM card is connected to the reader. The central computer calculates the Ksim derived from card information (ICC-ID) transmitted from the after-sales point, a component for generating the card unique identity (IMSI), the authentification key (Ki) and the personal unblocking key code (PUK), a unit for encoding the generated information using the key Ksim.

Thus, the system of cited prior art teaches and describe a system and a method to establish a trust relationship between a mobile communication terminal and a SIM chip card or the like, in order to secure exchanges between the card and the terminal as claimed in claims 1-22

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and dependent claims. Accordingly, rejections for Claims 1-22 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-22 are rejected under 35 U.S.C. 102(5) as being anticipated by Julin et al. U. S. Patent 5,557,679.

2. Regarding Claim 1, Julin teach and describe a method for establishing and managing a trust model between an identification module and a radio terminal , said method comprising: authenticating said radio terminal by said identification module, said authenticating being carried out by radio terminal authentication means that are provided either to said identification module by a mobile radio-telephony network at the time of an initialization or at the time of an updating, or to said radio terminal by the identification module; and controlling by said module at least one specific characteristic of the radio terminal , said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network (Fig.1-3, col.3line 20 to col.4line 26).

3. Claims 2-21 are rejected applied as above in rejecting claim 1 Furthermore, Julin teaches and describes a method of trust mode and personalization a chip card for mobile telephone

system, wherein:

As per Claim 2, said radio terminal authentication means present in the identification module are provided with a validity period that is limited by a determined expiration date, said authentication means being comprised of at least one authentication key (col.4 line 6 to line 16).

As per Claim 3, wherein said identification module comprises at least one of an SIM type chip card, an USIM card for third-generation networks or an equivalent card comprising in a memory the representative subscription data (Fig.3, col.3 line 20 to line 35).

As per Claim 4, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by secured exchange mechanisms based on authentication means initially available from the radio terminal (col.3 line 30 to line 40).

As per Claim 5, comprising at the time of said initialization or updating generating, carried out at least by said identification module, a trust key, said trust key being used by said module for encrypting at least data exchanged between the identification module and the radio terminal (col.3 line 55 to col.4 line 16).

As per Claim 6, wherein said initialization step of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by at least one of

said module, the mobile radio-telephony network or the radio terminal, following an expiration of the validity period of the key or at the time of initialization of the identification module (col.2 line 15 to line 33, col.2 line 44 to line 65).

As per Claim 7, wherein said authenticating comprises: utilization in the radio terminal of at least one first authentication key memorized in the radio terminal by at least on first authentication algorithm memorized in the radio terminal , said first key having a validity period limited by a predefined expiration date; utilization by the identification module of at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the radio terminal , said second key having a validity period limited by said predefined expiration date; comparing in the identification module the results obtained by said first and second authentication algorithms (col.3 line 63 to col.4 line 26).

As per Claim 8, the said authenticating comprises the utilization of said predefined expiration date (col.3 line 52 to col.4 line 26).

As per Claim 9, said initialization is initiated by a mobile radio-telephony network and also comprises: generation by the identification module of at least one of said first and second keys; a storage in the identification module of said second key; and transmission to the radio terminal by the identification module of said first key, said first key being encrypted by use of the trust key

(col.3 line 52 to col.4 line 16).

As per Claim 10, wherein said comparing is done between, a response produced by said first authentication algorithm, stored in memory in the radio terminal and transmitted to said identification module and, a response result, stored in memory in the identification module, produced by said second authentication algorithm (col.3 line 43 to col.4 line 26).

As per Claim 11, wherein said first key is an asymmetrical private key Ks and said second key being a public key Kp complementary to the first key (col.4 line 6 to line 16).

As per Claim 12, wherein said first key is symmetrical, said second key stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key (col.4 line 6 to line 26).

As per Claim 13, further comprising updating said first and second keys, initiated by the identification module prior to said predefined expiration, said updating including: authentication between the radio terminal and the identification module using said first and second keys; generation by an updating algorithm of the identification module of at least one updated key taking into account information for replacing at least one of said first and second keys; memorization in the identification module of the updated key for replacing said second key; +and transmission to the radio terminal by the identification module of the updated key analogue of said first key (col.3 line 52 to col.4 line 26).

As per Claim 14, wherein said updating further comprises the control of at least of one identifier of the radio terminal of the identification module (col.3 line 63 to col.4 line 6)

As per Claim 15, wherein an encryption of the key is carried out for said transmission to the radio terminal of the updated key analogue of the first key, said key encryption being done by said trust key (col.3 line 43 to col.4 line 26).

As per Claim 16, wherein the updating step also comprises: generation by the identification module of a new trust key after said authentication between radio terminal and module; memorization in the identification module of the new trust key; transmission to the radio terminal by the identification module of the newly generated trust key (col.3 line 43 to col.4 line 26).

As per Claim 17, wherein said updating is completed by a verification test comprising a return transmission on the part of the radio terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating (col.3 line 43 to col.4 line 26).

As per Claim 18, wherein said trust key is a symmetrical encryption/decryption key analogous to said symmetrical authentication key (col.3 line 43 to col.4 line 42).

As per Claim 19, wherein said trust key is an erasable session key (col.3 line 43 to line 63).

As per Claim 20, wherein a revocation step is carried out on the initiative of the identification module, of the radio terminal , or of the corresponding radio-telephony network, said revocation comprising the erasure in a memory of said identification module of at least said first key associated with the radio terminal (col.3 line 43 to col.4 line 26).

As per Claim 21, an identification module in a radio terminal comprising a device for memorizing at least one authentication key as well as at least one authentication algorithm, a calculation device for executing at least applying an authentication key to said authentication algorithm memorized in the identification module, a communication device for initiating a revocation and a revocation device for revoking said authentication key, a device for memorizing a specific characteristic of the radio terminal and a device for actuating an updating algorithm for updating said authentication key, the
communication device being capable of providing at least one authentication key to the radio terminal and receiving data send from a secured server of a mobile radiotelephony network (col.3 line 43 to col.4 line 26).

As per Claim 22, wherein said trust key is a symmetrical encryption/decryption key identical to said symmetrical authentication key (col.3 line 43 to col.4 line 26).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
April 14, 2008
/Syed Zia/
Primary Examiner, Art Unit 2131